Quantifying the nonlocality of GHZ quantum correlations by a bounded communication simulation protocol

Cyril Branciard[1] and Nicolas Gisin[2]
[1]*School of Mathematics and Physics, The University of Queensland, St Lucia, QLD 4072, Australia*
[2]*Group of Applied Physics, University of Geneva, 20 rue de l'Ecole-de-Médecine, CH-1211 Geneva 4, Switzerland*
(Dated: January 11, 2013)

The simulation of quantum correlations with alternative nonlocal resources, such as classical communication, gives a natural way to quantify their nonlocality. While multipartite nonlocal correlations appear to be useful resources, very little is known on how to simulate multipartite quantum correlations. We present the first known protocol that reproduces 3-partite GHZ correlations with bounded communication: 3 bits in total turn out to be sufficient to simulate all equatorial Von Neumann measurements on the 3-partite GHZ state.

When measurements are performed on several quantum systems in an entangled state, the statistics of the results may contain correlations that can't be simulated by shared local variables. Such correlations are called nonlocal. They can be identified by their capacity to violate some inequality: these so-called Bell inequalities are indeed satisfied by all correlations that can be explained by shared local variables [1].

The observation that quantum theory predicts nonlocal correlations is not new; it goes all the way back to the famous EPR argument [2]. Many experimental confirmations have been demonstrated all over the world during the last two decades of last century [3]. During the first ten years of this century, the interest for nonlocal correlations has shifted from mere skepticism and incredulity to more constructive questions. First, physicists raised the question of the power of nonlocal correlations for information processing; the main examples being "device-independent" quantum key distribution [4–6] and random number generation [7]. Second, theorists realized that quantum correlations, although possibly nonlocal, are never maximally nonlocal, hence the question "why is quantum theory not more nonlocal?" [8]; note the great advances since the original question "Why is quantum theory not local?".

Thirdly, and this is the topic of this letter, physicists and computer scientists tried to quantify nonlocality; that is, to treat nonlocality as a physical quantity. Indeed, the violation of a Bell inequality only proves that the correlations are not local, but doesn't tell us anything about how far from local they are, i.e. how much nonlocality they contain. Intuitively, a larger violation should signal more nonlocality. But this naïve approach is insufficient as some correlations may violate different Bell inequalities by different amounts. A quite natural measure of nonlocality is the number of classical bits that need to be communicated from one party to another in order to simulate the correlation. For local correlations, no communication is needed, as shared local variables suffice; hence local correlations have a "communication measure" equal to zero, as it should be. Let us stress that the idea is not to imagine that nature does use communication to produce nonlocal correlations, it is only to quantify the amount of nonlocality by the quantity of communication required to simulate the correlation.

That such a measure of nonlocality is natural is testified by the fact that it has been introduced by 3 independent papers [9–11]. More precisely, in this letter we adopt as a measure the number of bits communicated between all partners in the worst case [9, 10]. An alternative could be to count the number of bits sent on average [11, 12].

For the case of 2 qubits in a maximally entangled state, Toner and Bacon [13] proved that one single bit of communication suffices (if one restricts the analyses to projective Von Neumann measurements, as we do in this letter). Hence the nonlocality of two spin-$\frac{1}{2}$ particles in the singlet state is 1 bit. For the general case of 2 qubits in a partially entangled state it is known that 2 bits of communication are enough [13], though it is still unproven that one bit isn't sufficient. At first, one may think that the nonlocality of a partially entangled state shouldn't be larger than that of maximally entangled states, but this is not so clear once one realized the difficulty of simulating at the same time the nonlocal correlation and the nontrivial marginal probabilities [14, 15].

GHZ correlations. In this letter we consider 3-qubit GHZ quantum correlations and present the first known protocol to simulate such nonlocal correlations with bounded communication. This problem is the straightforward next step after the 2-qubit case; it attracted the attention of most of the specialists. After years of unsuccessful efforts, the feeling started to spread that it might be impossible with finite communication [16]. Some hope, however, appeared when Bancal et al. [17] presented a protocol with unbounded, but finite average communication. Moreover, a team recently presented a nonconstructive existence proof of a protocol with 6 bits of communication [18]; the proof turned out to be flawed, but the impulse was given!

More precisely, our goal is to simulate, with classical communication, the quantum correlations obtained by performing equatorial Von Neumann measurements on a 3-partite GHZ state. Namely: 3 parties, Alice, Bob and Charlie, each receive an input angle ϕ_A, ϕ_B and $\phi_C \in [0, 2\pi]$ (corresponding to a measurement setting on the equator of the Bloch sphere $\mathcal{S}^2$), and they must output binary outcomes $\alpha, \beta, \gamma \in \{+1, -1\}$, such that the expectation values satisfy

$$\langle \alpha\beta\gamma \rangle = \cos(\phi_A + \phi_B + \phi_C), \tag{1}$$

while all single- and bi-partite marginals vanish. Note that

although the choice of equatorial measurements is restrictive, these are enough to come up with the "GHZ paradox" [19]. We will show that our problem can be solved with finite communication. For that, we first introduce a protocol that provides "stronger" correlations, before showing how to adequately transform these and obtain the desired cosine correlations.

Simulation with classical communication. Consider the following protocol, that uses 3 bits of communication: 2 from Bob to Alice, and 1 from Charlie to Alice. The sign function below is defined as $\mathrm{sign}(x) = +1$ if $x \geq 0$, $\mathrm{sign}(x) = -1$ if $x < 0$.

Protocol 1. *Let Alice and Bob share two random vectors $\vec{\lambda}_1$ and $\vec{\lambda}_2$, uniformly distributed on the sphere $\mathcal{S}^2$, together with a random bit $\xi \in \{0,1\}$; let Alice and Charlie share a random variable φ_c, uniformly distributed on $[0, 2\pi]$.*

After reception of their measurement settings ϕ_A, ϕ_B and ϕ_C, the three parties proceed as follows:

0. Bob defines $\hat{b}$ to be the equatorial vector with azimuthal angle $\frac{\pi}{2} - 2\phi_B$; he calculates $\sigma_0 = \mathrm{sign}(\hat{b}\cdot\vec{\lambda}_1)\mathrm{sign}(\hat{b}\cdot\vec{\lambda}_2)$, and sends the bit $\tau_0 = \frac{1-\sigma_0}{2}$ to Alice. Alice and Bob can then both determine the azimuthal angle $\varphi_0 \in [0, 2\pi]$ of $\vec{\lambda}_0 = \vec{\lambda}_1 + (-1)^{\tau_0}\vec{\lambda}_2$; they calculate $\varphi_b = \frac{\varphi_0}{2} + \xi\pi \in [0, 2\pi]$.

1. Alice, Bob and Charlie define $\tilde{\phi}_A = \phi_A - \varphi_b - \varphi_c$, $\tilde{\phi}_B = \phi_B + \varphi_b$ and $\tilde{\phi}_C = \phi_C + \varphi_c$, respectively.

2. Bob calculates $\sigma_b = \mathrm{sign}(\sin 2\tilde{\phi}_B)$, and sends $\tau_b = \frac{1-\sigma_b}{2}$ to Alice; he outputs $\beta = \mathrm{sign}(\sin\tilde{\phi}_B)$.

Similarly, Charlie calculates $\sigma_c = \mathrm{sign}(\sin 2\tilde{\phi}_C)$, and sends $\tau_c = \frac{1-\sigma_c}{2}$ to Alice; he outputs $\gamma = \mathrm{sign}(\sin\tilde{\phi}_C)$.

3. Alice outputs $\alpha = \mathrm{sign}(\sin(-\tilde{\phi}_A - \tau_b\frac{\pi}{2} - \tau_c\frac{\pi}{2}))$.

Before analyzing the correlation given by Protocol 1, let us give an intuitive understanding of it. Forget for now the rather technical step 0 [20], and note that after step 1, one has $\tilde{\phi}_A + \tilde{\phi}_B + \tilde{\phi}_C = \phi_A + \phi_B + \phi_C$; the first two steps will ensure that the final tripartite correlation depends on the sum $\phi = \phi_A + \phi_B + \phi_C$ only, and that all marginals vanish. Assume now that $\tilde{\phi}_B, \tilde{\phi}_C \in [0, \pi]$ (and hence $\beta = \gamma = +1$); if this is not the case, Bob and Charlie can locally subtract π to $\tilde{\phi}_B$ or $\tilde{\phi}_C$ and flip their output, so that the correlation $E(\phi) = \langle\alpha\beta\gamma\rangle$ is unchanged – this is precisely why we ask them to output $\beta = \mathrm{sign}(\sin\tilde{\phi}_B)$ and $\gamma = \mathrm{sign}(\sin\tilde{\phi}_C)$. In step 2, Bob and Charlie tell Alice in which quadrant ($[0, \frac{\pi}{2}]$ or $[\frac{\pi}{2}, \pi]$) their angles $\tilde{\phi}_B$ and $\tilde{\phi}_C$ are. From this information, Alice knows in which half-circle $\tilde{\phi}_B + \tilde{\phi}_C$ is (more precisely, she knows $\mathrm{sign}(\sin(\tilde{\phi}_B + \tilde{\phi}_C))$ or $\mathrm{sign}(\cos(\tilde{\phi}_B + \tilde{\phi}_C))$, depending on whether $\tau_b = \tau_c$ or $\tau_b \neq \tau_c$); if $-\tilde{\phi}_A$ is in the same half-circle, she wants to obtain a good correlation with $\beta\gamma = +1$ (if by chance $-\tilde{\phi}_A = \tilde{\phi}_B + \tilde{\phi}_C$, she wants a perfect correlation!), and will thus output $\alpha = +1$; otherwise, she will output $\alpha = -1$; this corresponds precisely to step 3.

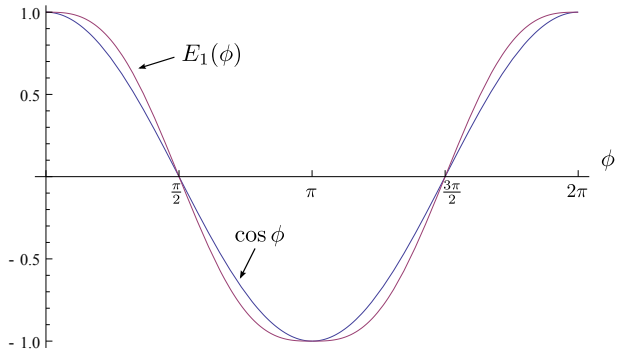

FIG. 1: Correlation $E_1(\phi) = E_1(\phi_A + \phi_B + \phi_C)$ obtained from Protocol 1, compared to the desired correlation $\cos(\phi)$.

As shown in Appendix A, Protocol 1 gives vanishing marginals, and the following 3-partite correlation $E_1(\phi) := \langle\alpha\beta\gamma\rangle$:

$$E_1(\phi) = \frac{32}{\pi^2}\sum_{n\geq 0}\frac{1}{(2n+1)^2}\,\frac{1}{4-(2n+1)^2}\cos\big((2n+1)\phi\big) = 1 - \frac{2\phi - \sin 2\phi}{\pi} \quad \text{for } \phi \in [0,\pi] \tag{2}$$

which, as already mentioned, only depends on the sum $\phi = \phi_A + \phi_B + \phi_C$.

$E_1(\phi)$ is shown on Figure 1. One can notice that it is "stronger" than the desired $\cos\phi$ correlation, in the sense that $|E_1(\phi)| \geq |\cos\phi|$ for all ϕ. Intuitively, one should be able to add some noise and weaken the correlation. However, weakening any given stronger correlation so as to obtain the desired cosine is not trivial, since this weakening must depend on ϕ and should in particular not weaken the extreme correlations for $\phi = 0$ and π. In fact, it seems that correlations must in general have quite specific properties for them to possibly be transformed to the desired cosine.

In order to do so, and starting from a 2π-periodic correlation function such that $E(0) = -E(\pi) = 1$, one can for instance try to mix correlations of the form $E\big((2m+1)\phi\big)$, with $m \in \mathrm{Z}$, as this will preserve the perfect (anti-)correlations for $\phi = 0$ and π. The following lemma gives a sufficient condition under which such a mixture can indeed give the desired cosine correlation [21].

Lemma 1. *Let $E(\phi)$ be a (2π-periodic, π-anti-periodic, even) real function with a Fourier decomposition of the form*

$$E(\phi) = \sum_{n\geq 0} e_{2n+1}\cos\big((2n+1)\phi\big), \tag{3}$$

such that

$$\begin{cases} e_1 > 0,\ e_{2n+1} \leq 0 \text{ for all } n \geq 1, \\ E(0) = \sum_{n\geq 0} e_{2n+1} = 1, \\ E''(0) = -\sum_{n\geq 0}(2n+1)^2 e_{2n+1} \leq 0. \end{cases} \tag{4}$$

Then $\cos\phi$ can be decomposed as

$$\cos\phi = \sum_{m\geq 0} p_{2m+1} E\big((2m+1)\phi\big), \tag{5}$$

with $p_{2m+1} \geq 0$ for all $m \geq 0$.

In particular, for $\phi = 0$, one gets $\sum_{m\geq 0} p_{2m+1} = 1$. The coefficients $p_{2m+1} \geq 0$ can thus be interpreted as probabilities, and the kind of "inverse Fourier decomposition" (5) is indeed a probabilistic mixture of correlations $E\big((2m+1)\phi\big)$.

A proof of Lemma 1 is given in Appendix B together with the explicit form of the p_{2m+1}. It is easy to check that E_1 satisfies the conditions (4). Hence, there exist coefficients $p_{2m+1} \geq 0$ such that $\sum_{m\geq 0} p_{2m+1} = 1$ and

$$\sum_{m\geq 0} p_{2m+1} E_1\big((2m+1)\phi\big) = \cos\phi. \qquad (6)$$

Consequently, and since $(2m+1)\phi_A + (2m+1)\phi_B + (2m+1)\phi_C = (2m+1)\phi$, the following protocol gives the desired cosine correlation and solves our problem, with the same 3 classical bits as in Protocol 1:

Protocol 2. *Let Alice, Bob and Charlie share, in addition to the randomness already introduced in Protocol 1, a random variable M that takes the value $M = 2m+1$ with probability p_{2m+1}, where $\{p_{2m+1}\}_{m\geq 0}$ are the coefficients of the decomposition (6).*

After reception of their measurement settings ϕ_A, ϕ_B and ϕ_C, the three parties run Protocol 1 with input angles $(2m+1)\phi_A, (2m+1)\phi_B$ and $(2m+1)\phi_C$, respectively.

Variants of our communication protocol. For convenience, let us from now on consider the equivalent 0/1 bit values corresponding to the 3 parties outputs in Protocol 1 (or 2): $a = \frac{1-\alpha}{2}, b = \frac{1-\beta}{2}$ and $c = \frac{1-\gamma}{2}$; the additions below will be modulo 2. Writing explicitly $a = a_{\tau_0\tau_b\tau_c}$ as a function of the classical communication (the bits τ_0, τ_b, τ_c) that Alice receives, one has

$$a_{\tau_0 11} = a_{\tau_0 00} + 1 \quad \text{and} \quad a_{\tau_0 01} = a_{\tau_0 10}\,. \qquad (7)$$

One can see that our communication protocol can actually be declined in different forms. In particular, Alice might not need to know the individual values of the bits τ_b and τ_c, but only their sum $\tau_{bc} = \tau_b + \tau_c$. Charlie's bit τ_c could for example be sent to Bob instead; Bob would then send τ_{bc} to Alice, who would output $a'_{\tau_0\tau_{bc}} = a_{\tau_0\tau_{bc}0}$; in the case when $\tau_b = \tau_c = 1$, the '+1' term in (7) can be introduced by Bob instead, who should output $b'_{\tau_c} = b + \tau_b\tau_c$. This thus induces a protocol 1', summarized as

$$\text{Prot. } 1' \;:\; \begin{cases} C \xrightarrow{\tau_c} B \xrightarrow{\tau_0,\tau_{bc}} A \\ c' = c\,,\; b'_{\tau_c} = b + \tau_b\tau_c\,,\; a'_{\tau_0\tau_{bc}} = a_{\tau_0\tau_{bc}0}\,, \end{cases}$$

With similar considerations, one can come up with many different variants with varied communication patterns, such as, for instance:

$$\text{Prot. } 1'' : \begin{cases} C \xrightarrow{\tau_c} B\,,\; B \xrightarrow{\tau_0} A \xrightarrow{\tau_a} B \\ c'' = c, a''_{\tau_0} = a_{\tau_0 00}, b''_{\tau_c\tau_a} = b + \tau_a\tau_b + \tau_a\tau_c + \tau_b\tau_c\,, \end{cases}$$

$$\text{Prot. } 1''' : \begin{cases} B \xrightarrow{\tau_b} C \xrightarrow{\tau_{bc}} A \xrightarrow{\tau_\alpha} B \\ c'''_{\tau_b} = c + \tau_b\tau_c,\; a'''_{\tau_{bc}} = a_{0\tau_{bc}0},\; b'''_{\tau_\alpha} = b + \tau_0\tau_\alpha\,, \end{cases}$$

with $\tau_a = a_{\tau_0 00} + a_{\tau_0 10}$ and $\tau_\alpha = a_{0\tau_{bc}0} + a_{1\tau_{bc}0}$. These variants and the original protocol look different, though they all require 3 bits of communication and lead to the same correlation. All of them have severe timing constraints (which is common for communication protocols): there are always some players that can't produce their output before some other partners receive their input and send them some information.

Simulation with PR boxes. An interesting alternative to measure nonlocality is to estimate the number of nonlocal PR-boxes [22] (some kind of "unit of nonlocality" [23]) required to simulate the correlations. Since the correlations we consider in this letter have no single- nor bi-partite marginals, all the variant communication protocols introduced above can be translated into PR-box based protocols [23]. Indeed, using (7) for the original version of Protocol 1, one can always decompose the sum $a + b + c$ as follows:

$$\begin{aligned} a_{\tau_0\tau_b\tau_c} + b + c \;=\; & a_{000} + b + c + \tau_0(a_{000}+a_{100}) \\ & + \tau_b(a_{000}+a_{010}) + \tau_0\tau_b(a_{000}+a_{010}+a_{100}+a_{110}) + \tau_b\tau_c \\ & + \tau_c(a_{000}+a_{010}) + \tau_0\tau_c(a_{000}+a_{010}+a_{100}+a_{110})\,. \qquad (8) \end{aligned}$$

The product terms in (8) can be generated by using nonlocal boxes: 5 PR-boxes can be used for the first 5 products (3 between Alice and Bob, 1 between Bob and Charlie and 1 between Alice and Charlie); the last product can be generated by a 3-partite GHZ-box, which can in turn be constructed from 3 PR-boxes [24]. Hence, a total of 8 PR-boxes suffices to simulate the tripartite GHZ correlations.

Interestingly, the variant communication protocols described above all lead to a PR-box based protocol with the same configuration of 8 PR-boxes, all used precisely in the same way. In addition to this invariance, and similarly to quantum correlations, the PR-box based protocol does not suffer from any timing constraint. Hence, it might be a more faithful tool to measure quantum nonlocality (at least, for correlations with vanishing marginals) – this question is quite general and would require further scrutinies beyond the scope of this letter. Note finally that reciprocally, simulating the PR boxes by communication gives a systematic way to generate different variants of our initial protocol, depending on which way we the communication goes.

Detection loophole. Another interesting connection is between our communication protocol and simulation models based on the detection loophole [12, 25]. For this connection let us start for instance from the last variant of the communication protocols. In the detection-loophole-based protocol, τ_b, τ_{bc} and τ_α are 3 additional shared random variables and each player outputs a bit if and only if the appropriate τ agrees with the bit he should send in the communication protocol. Hence, using variant 1"' of our protocol, the detection-loophole-based protocol simulates the GHZ correlations with "detection efficiencies" of 50% for Alice, Bob and Charlie. Other variant protocols can lead to detection-loophole-based protocols with asymmetric detection efficiencies.

Conclusion. We have proven that 3 bits of communication (or 8 PR-boxes) suffice to simulate 3-qubit GHZ equatorial

correlations; hence the nonlocality of these correlations is at most of 3 bits (8 PR-boxes). In the course of our derivation, we introduced a strategy to obtain a cosine correlation as a mixture of other ("harmonic") correlations, via Lemma 1, that we believe could be used in other contexts as well.

In this letter we considered correlations with vanishing single- and bi-partite marginals. If one considers also measurements on the GHZ state out of the equatorial plane [26], or if one considers other states such as biased GHZ-like states for instance, then the marginals will no longer be random, and simulating the entire probability distribution is likely to be significantly harder [15].

Two other important open problems are the questions of the optimality of our protocol and of its generalization to more parties. For 3 parties, since the GHZ correlations are truly 3-partite [27], a minimum of 2 bits is necessary to connect the 3 parties. We could find a 2-bit protocol (Protocol 1, without step 0, see [20]) that gives stronger correlations than $\cos\phi$ and that can approximate it to a very good accuracy, but not perfectly. For the N-partite case, it is easy to generalize protocol 1, again without step 0, using $(N-1)\log_2(N-1)$ bits of communication: divide the equator of the Bloch sphere into $2(N-1)$ equal sectors, let each of the $N-1$ last parties share a random angle φ_i with Alice, and tell her in which sector their angle $\tilde{\phi}_I = \phi_I + \varphi_i$ (modulo π) is. This leads again to a protocol giving stronger correlations than $\cos\phi$ (actually, stronger and stronger as N increases), with a number of bits that is asymptotically equivalent to the lower bound derived in [16] for the simulation of GHZ correlations ($N\log_2 N - 2N$). Unfortunately, we did not find a generalization that would give a correlation satisfying the assumptions of Lemma 1, so that the exact cosine correlation could then be obtained as in Protocol 2.

These observations lead us to formulate the following question: should we understand a "stronger" correlation as being "more non-local"? If our goal is to quantify the power of nonlocality as a resource for achieving some information processing task, then the next question follows: is there any (useful) task, for which a stronger correlation might actually be less powerful than a weaker one? If this is not the case, then one could be happy with simulation protocols that give stronger correlations than the desired ones, and for this operational interpretation of the nonlocality measure, we could conclude that the nonlocality of the 3-partite GHZ correlations is at most 2 bits (or 3 PR-boxes), and that of the $N-$partite GHZ correlations is at most $(N-1)\log_2(N-1)$ bits.

Nonlocal correlations are fascinating. First, because they can't be simulated by mere shared local variables; next, because even if finite communication is allowed, their simulation remains tedious and quite artificial. Hence, simulating in particular quantum nonlocal correlations with classical resources, like shared local variables and communication, looks in general extremely difficult. This underlines the power of nonlocal correlations. Yet, such simulations seem to give a good measure of nonlocality (whether we are interested in the exact simulation or in the "operational nonlocality" measure), possibly the best together with PR-box based simulations, and provide the only story that takes place in space and time about how they could occur.

We acknowledge discussions with G. Brassard, M. Kaplan, S. Pironio and I. Villanueva. This work profited from financial support from the Australian Research Council Centre of Excellence for Quantum Computer Technology, the Swiss NCCR-QP and NCCR-QSIT, and the EU AG-QORE.

[1] J. Bell, *Speakable and unspeakable in quantum mechanics* (Cambridge University Press, 2004), 2nd ed.
[2] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[3] A. Aspect, Nature **398**, 189 (1999).
[4] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[5] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[6] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).
[7] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, et al., Nature **464**, 1021 (2010).
[8] S. Popescu, Nature Physics **2**, 507 (2006).
[9] T. Maudlin, *Proceedings of the 1992 Meeting of the Philosophy of Science Association* (D. Hull, M. Forbes, and K. Okruhlik, Philosophy of Science Association, East Lansing, MI, 1992), vol. 1, pp. 404–417.
[10] G. Brassard, R. Cleve, and A. Tapp, Phys. Rev. Lett. **83**, 1874 (1999).
[11] M. Steiner, Phys. Lett. A **270**, 239 (2000).
[12] N. Gisin and B. Gisin, Phys. Lett. A **260**, 323 (1999).
[13] B. F. Toner and D. Bacon, Phys. Rev. Lett. **91**, 187904 (2003).
[14] A. A. Méthot and V. Scarani, Quant. Inf. Comp. **7**, 157 (2007).
[15] N. Brunner, N. Gisin, S. Popescu, and V. Scarani, Phys. Rev. A **78**, 052111 (2008).
[16] A. Broadbent, P.-R. Chouha, and A. Tapp, Third International Conference on Quantum, Nano, and Micro Technologies pp. 59–62 (2009).
[17] J.-D. Bancal, C. Branciard, and N. Gisin, Adv. Math. Phys. **2010**, Article ID 293245 (2010).
[18] C. Palazuelos, D. Perez-Garcia, and I. Villanueva, arXiv:1006.5318 (2010).
[19] D. M. Greenberger, M. A. Horne, and A. Zeilinger, *Bells Theorem, Quantum Theory, and Conceptions of the Universe* (ed. M. Kafatos, Kluwer Academic, Dordrecht, Holland, 1989), pp. 69–72.
[20] Step 0 allows Alice and Bob to sample their shared random variable φ_b [28] so that it follows an appropriate sine distribution (see Appendix A). Note that we could define a similar protocol as Protocol 1, but without step 0, and starting directly with φ_b uniformly distributed on $[0, 2\pi]$. This simpler protocol, that requires only 2 bits of communication (or 3 PR-boxes, 1 between each pair of parties), would also give a stronger correlation $E_0(\phi) = \frac{32}{\pi^3}\sum_{n\geq 0}\frac{(-1)^n}{(2n+1)^3}\cos\big((2n+1)\phi\big)$ $(= 1 - \frac{4\phi^2}{\pi^2}$ for $\phi \in [0, \frac{\pi}{2}])$ than $\cos\phi$. However, $E_0(\phi)$ does not satisfy the assumptions of Lemma 1; by mixing correlations of the form $E_0\big((2m+1)\phi\big)$, one can approximate the cosine correlation with a very good accuracy, but not exactly.

[21] It is interesting to note the similarities of our approach here with that presented in [29], and in particular to compare the assumptions of our Lemma 1 with those of Lemma 3.1 there. As in [29], our lemma only gives sufficient conditions for the decomposition (5) to exist, with $p_{2m+1} \geq 0$; it is not clear to us which are the necessary and sufficient conditions for the conclusion of Lemma 1 to be reached. In particular, the fact that $E(\phi)$ is stronger than $\cos\phi$ is actually not a necessary condition (for a counterexample, consider for instance $E(\phi) = 1.04\cos\phi - 0.04\cos 5\phi$).
[22] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[23] J. Barrett and S. Pironio, Phys. Rev. Lett. **95**, 140401 (2005).
[24] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, Phys. Rev. A **71**, 022101 (2005).
[25] P. M. Pearle, Phys. Rev. D **2**, 1418 (1970).
[26] For non-equatorial measurements, our protocol fails to reproduce the non-vanishing marginals. However, if one is not interested in the marginals but only wants to simulate the tripartite correlation term $\langle\alpha\beta\gamma\rangle = \sin\theta_A \sin\theta_B \sin\theta_C \cos\phi$ (where θ_A, θ_B and θ_C are the zenith angles of the 3 measurement settings in $\mathcal{S}^2$), then our protocol can be used, as each party can locally add the appropriate amount of noise to introduce the factors $\sin\theta_I$. Note also that if no more than one party performs a non-equatorial measurement, the marginals are in fact still random, and the full correlation can again be simulated.
[27] G. Svetlichny, Phys. Rev. D **35**, 3066 (1987).
[28] J. Degorre, S. Laplante, and J. Roland, Phys. Rev. A **72**, 062314 (2005).
[29] O. Regev and B. Toner, SIAM Journal on Computing **39**, 1562 (2009), preliminary version in FOCS'07.

Appendix A: Calculation of $E_1(\phi)$

In this Appendix we analyze the correlation obtained with Protocol 1. We first introduce two useful lemmas.

Lemma 2. *Let $\vec{a}$ be a vector on the equator of $\mathcal{S}^2$, with azimuthal angle ϕ_A. Consider two random vectors $\vec{\lambda}_1, \vec{\lambda}_2$ uniformly distributed on the half sphere $\mathcal{S}^+(\vec{a}) = \{\vec{\lambda} \in \mathcal{S}^2 \mid \vec{a}\cdot\vec{\lambda} \geq 0\}$, and define $\vec{\lambda} = \frac{\vec{\lambda}_1+\vec{\lambda}_2}{||\vec{\lambda}_1+\vec{\lambda}_2||}$. Then the azimuthal angle $\varphi \in [\phi_A - \frac{\pi}{2}, \phi_A + \frac{\pi}{2}]$ of $\vec{\lambda}$ is distributed according to*

$$\rho(\varphi) = \frac{1}{2}\cos(\varphi - \phi_A). \tag{9}$$

Alternatively, if one doesn't want to restrict *a priori* φ to be in $[\phi_A - \frac{\pi}{2}, \phi_A + \frac{\pi}{2}]$, one can write, for any $\varphi \in [0, 2\pi]$ (or any real interval with amplitude 2π),

$$\rho(\varphi) = \max(0, \frac{1}{2}\cos(\varphi - \phi_A)). \tag{10}$$

Proof of Lemma 2:

Denote by $\rho_{\mathcal{S}^2}$ and $\rho_{\mathcal{S}^+}$ the uniform distributions on $\mathcal{S}^2$ and $\mathcal{S}^+(\vec{a})$, respectively. For another vector $\vec{b}$ on the equator of $\mathcal{S}^2$, with azimuthal angle ϕ_B, let's calculate:

$$\begin{aligned}
&\mathcal{I} \\
&:= \int_{\mathcal{S}^+(\vec{a})} \rho_{\mathcal{S}^+}(\vec{\lambda}_1)\,\mathrm{d}\vec{\lambda}_1 \int_{\mathcal{S}^+(\vec{a})} \rho_{\mathcal{S}^+}(\vec{\lambda}_2)\,\mathrm{d}\vec{\lambda}_2\ \mathrm{sign}\big(\vec{b}\cdot(\vec{\lambda}_1+\vec{\lambda}_2)\big) \\
&= \int_{\mathcal{S}^2} \rho_{\mathcal{S}^2}(\vec{\lambda}_1)\,\mathrm{d}\vec{\lambda}_1 \int_{\mathcal{S}^2} \rho_{\mathcal{S}^2}(\vec{\lambda}_2)\,\mathrm{d}\vec{\lambda}_2\ \mathrm{sign}\big(\vec{b}\cdot(\sigma_1\vec{\lambda}_1+\sigma_2\vec{\lambda}_2)\big) \\
&= \int_{\mathcal{S}^2} \rho_{\mathcal{S}^2}(\vec{\lambda}_1)\,\mathrm{d}\vec{\lambda}_1 \int_{\mathcal{S}^2} \rho_{\mathcal{S}^2}(\vec{\lambda}_2)\,\mathrm{d}\vec{\lambda}_2\ \sigma_1\,\mathrm{sign}\big(\vec{b}\cdot(\vec{\lambda}_1+\sigma_1\sigma_2\vec{\lambda}_2)\big)
\end{aligned}$$

with $\sigma_i = \mathrm{sign}(\vec{a}\cdot\vec{\lambda}_i)$. The last integrals were calculated by Toner and Bacon in [13], and were found to be equal to $\vec{a}\cdot\vec{b} = \cos(\phi_B - \phi_A)$.

Now, the term $\mathrm{sign}\big(\vec{b}\cdot(\vec{\lambda}_1+\vec{\lambda}_2)\big)$ in the definition of $\mathcal{I}$ above is simply equal to $\mathrm{sign}\big(\cos(\varphi - \phi_B)\big)$, so that the integral is also equal to

$$\mathcal{I} = \cos(\phi_B - \phi_A) = \int_{\phi_A-\frac{\pi}{2}}^{\phi_A+\frac{\pi}{2}} \rho(\varphi)\,\mathrm{d}\varphi\ \mathrm{sign}\big(\cos(\varphi - \phi_B)\big)\,. \tag{11}$$

Defining $R(\phi) = \int_{\phi_A-\frac{\pi}{2}}^{\phi} \rho(\varphi)\,\mathrm{d}\varphi$ (with $R(\phi_A + \frac{\pi}{2}) = 1$ due to normalization), the explicit calculation of (11) leads to

$$\cos(\phi_B - \phi_A) = 1 - 2R(\phi_B - \frac{\pi}{2}) \quad \text{if} \quad \phi_A \leq \phi_B \leq \phi_A + \pi\,,$$
$$\cos(\phi_B - \phi_A) = 2R(\phi_B + \frac{\pi}{2}) - 1 \quad \text{if} \quad \phi_A - \pi \leq \phi_B \leq \phi_A\,.$$

With now $\varphi = \phi_B \mp \frac{\pi}{2}$, both equalities above give

$$2R(\varphi) - 1 = \sin(\varphi - \phi_A) \quad \text{for} \quad \phi_A - \frac{\pi}{2} \leq \varphi \leq \phi_A + \frac{\pi}{2}\,.$$

After differentiation, one obtains

$$\rho(\varphi) = \frac{1}{2}\cos(\varphi - \phi_A).$$

□

Lemma 3. *After step 0 of Protocol 1, $\varphi_b \in [0, 2\pi]$ is distributed according to*

$$\rho(\varphi_b) = \frac{1}{4}|\sin 2(\varphi_b + \phi_B)|\,. \tag{12}$$

Proof of Lemma 3:

We now use the notation $\sigma_i = \mathrm{sign}(\hat{b}\cdot\vec{\lambda}_i)$.

Suppose first that $\sigma_1 = +1$. Then $\vec{\lambda}_0 = \vec{\lambda}_1 + \sigma_1\sigma_2\vec{\lambda}_2 = \sigma_1\vec{\lambda}_1 + \sigma_2\vec{\lambda}_2$ is the sum of two vectors uniformly distributed on $\mathcal{S}^+(\hat{b})$. From Lemma 2, the distribution of its azimuthal angle $\varphi_0 \in [0, 2\pi]$ is

$$\begin{aligned}
\rho_+(\varphi_0) &= \max\big(0, \frac{1}{2}\cos(\varphi_0 - (\frac{\pi}{2} - 2\phi_B))\big) \\
&= \max\big(0, \frac{1}{2}\sin(\varphi_0 + 2\phi_B)\big)\,.
\end{aligned}$$

In the case where $\sigma_1 = -1$, $\vec{\lambda}_0 = \vec{\lambda}_1 + \sigma_1\sigma_2\vec{\lambda}_2 = -\sigma_1\vec{\lambda}_1 - \sigma_2\vec{\lambda}_2$ is the sum of two vectors uniformly distributed on $\mathcal{S}^+(-\hat{b})$. The distribution of its azimuthal angle $\varphi_0 \in [0, 2\pi]$ is

$$\rho_-(\varphi_0) = \max\big(0, \frac{1}{2}\sin(\varphi_0 + 2\phi_B + \pi)\big)\,.$$

As Alice and Bob ignore the individual value of σ_1 ($= \pm 1$ with equal probabilities), the overall distribution of φ_0 is

$$\rho_0(\varphi_0) = \frac{1}{2}\big(\rho_+(\varphi_0) + \rho_-(\varphi_0)\big) = \frac{1}{4}|\sin(\varphi_0 + 2\phi_B)|\,.$$

The distribution of $\varphi_b^0 = \frac{\varphi_0}{2} \in [0, \pi]$ is then

$$\rho_b^0(\varphi_b^0) = 2\rho_0(2\varphi_b^0) = \frac{1}{2}|\sin(2\varphi_b^0 + 2\phi_B)|\,,$$

and after adding $\xi\pi$, with $\xi \in \{0, 1\}$ random, the distribution of $\varphi_b = \varphi_b^0 + \xi\pi \in [0, 2\pi]$ is finally

$$\rho(\varphi_b) = \frac{1}{4}|\sin(2\varphi_b + 2\phi_B)|\,.$$

□

Let us now calculate the correlation obtained with Protocol 1. One can, for simplicity, directly integrate over the variables $\tilde{\phi}_B = \phi_B + \varphi_b$ and $\tilde{\phi}_C = \phi_C + \varphi_c$; from Lemma 3, $\tilde{\phi}_B$ is distributed according to $\rho(\tilde{\phi}_B) = \frac{1}{4}|\sin(2\tilde{\phi}_B)|$, while $\tilde{\phi}_C$ is uniformly distributed on $[0, 2\pi]$. One can easily check that the single- and bi-partite marginals vanish; the tripartite correlation writes

$$\langle\alpha\beta\gamma\rangle = \int_0^{2\pi} \mathrm{d}\tilde{\phi}_B \frac{1}{4}|\sin(2\tilde{\phi}_B)| \int_0^{2\pi} \frac{\mathrm{d}\tilde{\phi}_C}{2\pi} \operatorname{sign}(\sin\tilde{\phi}_B)\operatorname{sign}(\sin\tilde{\phi}_C) \times \operatorname{sign}\big(\sin(\tilde{\phi}_B + \tilde{\phi}_C - \phi - \tau_b(\tilde{\phi}_B)\frac{\pi}{2} - \tau_c(\tilde{\phi}_C)\frac{\pi}{2})\big),$$

and only depends on $\phi = \phi_A + \phi_B + \phi_C$.

Using the periodicity of the integrand function, one obtains

$$E_1(\phi) \;:=\; \langle\alpha\beta\gamma\rangle = \frac{2}{\pi}\int_0^{\frac{\pi}{2}} \mathrm{d}\tilde{\phi}_B \int_0^{\frac{\pi}{2}} \mathrm{d}\tilde{\phi}_C\; \sin(2\tilde{\phi}_B) \times \operatorname{sign}\big(\sin(\tilde{\phi}_B + \tilde{\phi}_C - \phi)\big).$$

It is convenient to use the Fourier decomposition $\operatorname{sign}(\sin x) = \frac{4}{\pi}\sum_{n\geq 0}\frac{1}{2n+1}\sin\big((2n+1)x\big)$ to calculate the integrals. One then easily gets

$$E_1(\phi) = \frac{32}{\pi^2}\sum_{n\geq 0}\frac{1}{(2n+1)^2}\,\frac{1}{4-(2n+1)^2}\cos\big((2n+1)\phi\big)\,. \tag{13}$$

One can finally check that $E_1(\phi)$ can also be written as $E_1(\phi) = 1 - \frac{2\phi - \sin 2\phi}{\pi}$ for $\phi \in [0, \pi]$, from which the full function can be obtained by symmetry and periodicity.

Appendix B: Proof of Lemma 1

Assume that $E(\phi)$ satisfies the assumptions (3-4). Define $p_1 = \frac{1}{e_1}$ and, for $m \geq 1$,

$$p_{2m+1} \;=\; -\frac{1}{e_1}\sum_{k=0}^{m-1}\sum_{n=1}^{m} p_{2k+1}e_{2n+1}\delta_{(2k+1)(2n+1),2m+1} \tag{14}$$

(with $\delta_{i,j} = 1$ if $i = j$, $\delta_{i,j} = 0$ otherwise).

Note that these coefficients p_{2m+1} are non-negative. We will show that they lead to the decomposition (5). The proof is partly inspired by that of Lemma 3.1 in [29]; we divide it into 3 steps.

- *Step 1:* We first prove that the coefficients p_{2m+1} can be written as

$$p_{2m+1} = \frac{1}{e_1}\sum_{\ell_3,\ell_5,\ldots}\frac{(\ell_3+\ell_5+\ldots)!}{\ell_3!\ell_5!\ldots}\Big(-\frac{e_3}{e_1}\Big)^{\ell_3}\Big(-\frac{e_5}{e_1}\Big)^{\ell_5}\cdots\,, \tag{15}$$

where the (finite) sum is taken over all non-negative integers $\ell_3, \ell_5, \ldots$ such that $3^{\ell_3}\times 5^{\ell_5}\times\cdots = 2m+1$.

We prove it by induction. Note that (15) holds for $m = 0$; suppose p_{2k+1} can be written as in (15) for all $k < m$. Then, with the notation $i|j$ meaning "i divides j", one can write

$$\begin{aligned} p_{2m+1} \;&=\; -\frac{1}{e_1}\sum_{\substack{n=1,\\ \text{s.t. } 2n+1|2m+1}}^{m} e_{2n+1}\, p_{\frac{2m+1}{2n+1}} \\ &=\; \frac{1}{e_1}\sum_{\substack{n=1,\\ \text{s.t. } 2n+1|2m+1}}^{m}\Big(-\frac{e_{2n+1}}{e_1}\Big)\sum_{\substack{\ell_3,\ell_5,\ldots\\ \text{s.t. } 3^{\ell_3}5^{\ell_5}\cdots=\frac{2m+1}{2n+1}}}\frac{(\ell_3+\ell_5+\ldots)!}{\ell_3!\ell_5!\ldots}\Big(-\frac{e_3}{e_1}\Big)^{\ell_3}\Big(-\frac{e_5}{e_1}\Big)^{\ell_5}\cdots \end{aligned}$$

$$p_{2m+1} = \frac{1}{e_1} \sum_{\substack{n=1,\\ \text{s.t. } 2n+1|2m+1}}^{m} \sum_{\substack{\ell_3,\dots\ell_{2n+1},\dots\\ \text{s.t. } 3^{\ell_3}\dots(2n+1)^{\ell_{2n+1}+1}\dots=2m+1}} \frac{(\ell_3+\dots+\ell_{2n+1}+\dots)!}{\ell_3!\dots\ell_{2n+1}!\dots} \left(-\frac{e_3}{e_1}\right)^{\ell_3} \dots \left(-\frac{e_{2n+1}}{e_1}\right)^{\ell_{2n+1}+1} \dots$$

$$= \frac{1}{e_1} \sum_{\substack{n=1,\\ \text{s.t. } 2n+1|2m+1}}^{m} \sum_{\substack{\ell_3,\ell_5,\dots\\ \text{s.t. } 3^{\ell_3}5^{\ell_5}\dots=2m+1}} \frac{\ell_{2n+1}}{\ell_3+\ell_5+\dots} \frac{(\ell_3+\ell_5+\dots)!}{\ell_3!\ell_5!\dots} \left(-\frac{e_3}{e_1}\right)^{\ell_3} \left(-\frac{e_5}{e_1}\right)^{\ell_5} \dots$$

where we relabeled $(\ell_{2n+1}+1) \to \ell_{2n+1}$. After exchanging the two sums, and using the fact that $\sum_{n=1}^{m} \frac{\ell_{2n+1}}{\ell_3+\ell_5+\dots} = 1$, one obtains (15) as desired.

- *Step 2:* We now show that $\sum p_{2m+1}$ converges absolutely.

Eq. (15) can be written as

$$p_{2m+1} = \tfrac{1}{e_1} \tfrac{1}{(2m+1)^{3/2}} \textstyle\sum_{\ell_3,\ell_5,\dots} \frac{(\ell_3+\ell_5+\dots)!}{\ell_3!\ell_5!\dots} \times \left(-\tfrac{3^{3/2}e_3}{e_1}\right)^{\ell_3} \left(-\tfrac{5^{3/2}e_5}{e_1}\right)^{\ell_5} \dots .$$

All the terms in the sum are non-negative. If one extends the sum to all integers $\ell_3, \ell_5, \dots$, one gets the upper bound

$$p_{2m+1} \le \tfrac{1}{e_1} \tfrac{1}{(2m+1)^{3/2}} \textstyle\sum_{L=0}^{\infty} \sum_{\ell_3,\ell_5,\dots} \frac{L!}{\ell_3!\ell_5!\dots} \times \left(-\tfrac{3^{3/2}e_3}{e_1}\right)^{\ell_3} \left(-\tfrac{5^{3/2}e_5}{e_1}\right)^{\ell_5} \dots$$

where in the second sum, the indices are now such that $\ell_3 + \ell_5 + \dots = L$.

From the assumptions (4), $\sum (2n+1)^{3/2}(-e_{2n+1}) \le \sum (2n+1)^2(-e_{2n+1})$ converges absolutely, and one can apply the multinomial theorem to calculate the inner sum; one finds that this sum is $(C_{3/2})^L$, where $C_{3/2} = \sum_{n=1}^{\infty} \big(-\frac{(2n+1)^{3/2}e_{2n+1}}{e_1} \big)$.

Now, $0 \le \sum_{n=1}^{\infty} (2n+1)^{3/2}(-e_{2n+1}) < \sum_{n=1}^{\infty} (2n+1)^2(-e_{2n+1}) \le e_1$ by assumption[1]; hence $0 \le C_{3/2} < 1$, and therefore one gets

$$0 \le p_{2m+1} \le \tfrac{1}{e_1} \tfrac{1}{(2m+1)^{3/2}} \textstyle\sum_{L=0}^{\infty} (C_{3/2})^L = \tfrac{1}{e_1} \tfrac{1}{1-C_{3/2}} \tfrac{1}{(2m+1)^{3/2}} ,$$

which implies that $\sum p_{2m+1}$ converges absolutely.

Note also that the assumptions (4) imply that $\sum e_{2n+1}$ converges absolutely as well.

[1] The strict inequality in what precedes should actually be replaced by an equality in the case where $e_1 = 1$ and $e_{2n+1} = 0$ for all $n \ge 1$. But the conclusion still holds in that trivial case.

- *Step 3:* Conclusion

The fact that $\sum p_{2m+1}$ and $\sum e_{2n+1}$ are absolutely convergent allows one to calculate the following infinite sums:

$$\sum_{m\ge 0} p_{2m+1} E\big((2m+1)\phi\big)$$
$$= \sum_{m\ge 0} p_{2m+1} \sum_{n\ge 0} e_{2n+1} \cos\big((2m+1)(2n+1)\phi\big)$$
$$= \sum_{k\ge 0} \Big(\sum_{m=0}^{k} \sum_{n=0}^{k} p_{2m+1} e_{2n+1} \delta_{(2m+1)(2n+1),2k+1} \Big) \cos\big((2k+1)\phi\big) .$$

By definition (14), the double sum inside the brackets is equal to $\delta_{k,1}$, and one obtains, as desired,

$$\sum_{m\ge 0} p_{2m+1} E\big((2m+1)\phi\big) = \cos(\phi) . \qquad (16)$$

□